payments and crypto network

## FCA Cryptoasset registrations

## Guide 4: FCA feedback on applications (Part 2)

Guidance is provided for firms and is not intended as legal advice.

Background

The FCA are the anti-money laundering ("AML") and counter-terrorist financing ("CTF") supervisor of UK cryptoasset businesses under the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 ("MLR"). Firms proposing to conduct cryptoasset activities in the UK must register with the FCA beforehand. Cryptoasset firms are often referred to as Virtual Asset Service Providers ("VASP").

Individuals and businesses have to register with the FCA for AML and CTF purposes, if they are carrying on cryptoasset activities that are:

(i) within scope of the MLR

(ii) if this activity is in the course of business; and

(iii) if the activity is carried on in the United Kingdom.

The FCA recommend that legal advice is sought regarding whether your business requires registration before engaging in the application process.

A cryptoasset registration is different from authorisation as an Electronic Money Institution ("EMI") or Payment Institution ("PI"). An EMI or PI wishing to undertake cryptoasset activities in the UK will still need to register with the FCA as a separate application process.

The FCA have published feedback on *"good and poor quality applications*" – their findings are the subject of this Guide (which is the second of two guides addressing their Feedback).

FCA feedback on *"good and poor quality applications"*

In September 2023 the FCA published feedback discussing what elements they deem to be associated with *"good quality"* and *"poor quality"* applications that have been made in accordance with the requirement to register cryptoasset firms under the MLR.

The FCA intend that the feedback helps improve the quality of future applications in order to help make the process as simple and efficient as possible. All firms intending to submit an application for registration would be well advised to review the FCA's feedback in addition to the guidance published on their website. Applicants should consider the registration rates, as published by the FCA, which are 7% (based on the 12 months to 1 September 2023) when considering the amount of background research they undertake before preparing an application for registration and the resources that are allocated to the process.

The FCA provided their feedback in a number of distinct areas, each of which are addressed below.

## 1. Business plan

A Regulatory Business Plan ("RBP") would be prepared as the key part of the submission and the 'business plan' content discussed here, along with other descriptions, should be included therein.

### Service description and supporting flow of funds diagram(s)

The FCA state that the applicant's business plan should include *"details of its business model, roles and responsibilities of business partners (such as service providers, brokers, introducers, sub-custodians and outsourcing partners), sources of liquidity, detailed customer journey and flow-of-funds diagram for both fiat and cryptoassets flows"*.

The agreement of a service description and a clear understanding of the permissions required will be key to a successful application. Applicants should also understand how the proposed services will develop over a three-year period in order to (i) assist with the preparation of a clear and concise service description, (ii) ensure that the permissions being applied for are appropriate (so as not to have to come back for additional permissions in the near future, if at all possible), and (iii) to help prepare the three-year financial forecast. These two guides should help:

- **Applications for Authorisation: Guide 1 – Permissions**
- **Applications for Authorisation: Guide 2 - Service development**

The application should also explain how the proposed cryptoasset activities relate to the MLRs, i.e. the basis for having to seek registration in the UK and the cryptoasset activities that will be provided and permissions required. This first guide will assist set the context:

- **Cryptoasset registration: Guide 1 - Requirement to register**

### Financial forecast

The FCA require applicants to submit a financial forecast for a period of three financial years. FCA feedback specifically references unrealistic forecasts relating to *"staffing, marketing plans, customer breakdown or any other component of the plan"*. It is advisable to build a reasonable financial forecast based on the descriptions of the services, realistic development plans, organisational structure, etc. that are included in the application (specifically the RBP). The following guide provides helpful information on the preparation of a financial forecast to support an application:

- **Applications for Authorisation: Guide 8 - Financial forecast**

### Business plan content

The FCA's feedback also state that applicants should not submit business plans that *"focus only on the business model and commercial aspects without any description of its compliance oversight, risk mitigation and financial controls, especially for its cryptoasset holdings"*. They highlight examples, including:

- Whether there are arrangements to segregate its customers' fiat or cryptoassets with its own fiat or cryptoassets

- Whether the customer flow of funds and cryptoassets is unambiguous,
- Clarity on the applicant's responsibilities regarding its custodial holdings, and
- Transparency on reserves.

## 2. Comprehensive description of products and services

The FCA highlight that applications should include *"a comprehensive and accurate description of the applicant's products and services"*. Whilst the issue of service descriptions has already been referenced above, the FCA elaborate on the requirement to include:

- Cryptoasset token vetting policy
- Detailed descriptions of dependencies on external ecosystems for liquidity, custodian services, and
- Underlying smart contracts / DeFi implementations.

The service description should also include *"a description of any cryptoassets native to, or otherwise associated with, the applicant and relevant whitepapers, token classification and functionalities assigned within the business"*.

A clear service description forms the basis of the application and would logically be the starting point for the preparation of the application and development of the arrangements and operations on which the business will be based.

## 3. Risk assessment and management

The FCA require applicants to demonstrate *"a thorough understanding of the risks from dealing in cryptoassets and design a business wide risk assessment that is tailored to its business model"*.

In addition to the AML / CTF risks, the FCA require the risk assessment to identify and assess any proliferation financing risks relevant to the business. The following guide provides general advice on developing risk management arrangements (albeit in the context of preparing an application for authorisation as an EMI or PI business):

- **Applications for Authorisation: Guide 6 - Risk management arrangements**

The FCA state that they will not approve an application where the applicant has *"an incorrect understanding of the risks associated with cryptoasset products or it has not considered the additional risks from combining new cryptoasset-related services or products with its ongoing business model"*.

In developing the risk management approach (i.e. a risk management framework, including a methodology for assessing risk) it would be sensible to prepare a Risk Register. Whilst the focus of the FCA's feedback is related to the management of financial crime risks, businesses should consider risks throughout the business, i.e. on an enterprise-wide basis. These should be categorised and included in the Risk Register. The subject of developing a risk management framework is discussed in this guide:

- **Risk Management Arrangements: Guide 2 - Risk management framework**

The preparation of a Risk Register, which would operate at the centre of the risk management framework, will enable the business to record identified risks, and their associated mitigating controls, as well as coordinate the performance of risk assessments.

The process of preparing a Risk Register will assist the business explain, in the application, the risks that are related to the proposed cryptoasset activities and how these are mitigated. The Risk Register will have operational value for the business and its preparation will focus attention on the issue of risk management in practical and real terms – this will be reflected in the quality of the application content (see also next section of FCA feedback). The subject of preparing a Risk Register is covered in the guide:

- **Risk Management Arrangements: Guide 3 - Building a Risk Register**

## 4. Policies, systems & controls

Mitigation of risks

The theme of risk management continues with the FCA's feedback on the quality of applicant's *"policies, systems and controls"*. The FCA expect applicants to have policies, systems and controls in place to *"appropriately manage and mitigate the risks identified in the business wide risk assessment"*. As described above, the process of preparing a Risk Register will focus attention on exactly this issue.

The description of other control areas, e.g. governance arrangements and the internal control environment, that are included in the RBP should link to the risk management activities, e.g. include details on how these areas contribute to the mitigation of the identified risks.

The FCA also state that they *"expect applicants to adequately evidence their assessment of the strength of these controls"*. Again, the preparation of a Risk Register will help applicants to produce this evidence, i.e. the assessment of the Inherent Risk (before the application of mitigating controls) and the Residual Risk (after the application of mitigating controls). The FCA provide some specific examples where controls will be required:

- Reliance on external ecosystems for liquidity
- Considerations on the interoperability of the applicant's products
- Market-maker related risk mitigation
- Native token trading
- White labelling services,
- Unusual B2B models,
- Sub-custodian services, or
- Reliance on peer-to-peer platforms.

Financial crime controls

The FCA state that they will not approve an application where there is *"an underdeveloped AML framework or a weak governance structure"*.

The FCA highlight issues where the applicant:

- has no clear methodology for risk-scoring its customers
- does not consider all relevant factors
- allows customer transactions before it has completed customer due diligence, and
- does not understand the enhanced due diligence triggers.

Further, the FCA state, and not unreasonably so, that applicants *"should not submit generic / off-the-shelf policies and procedures that do not align with their business model or that contain obsolete documents not designed for or adapted to the proposed cryptoasset activities"*.

It is critical that the arrangements described in the application are developed specifically for the business. If they are generic or outdated, it is very likely that the applicant will not have properly thought through the implications that regulatory requirements will have on the business. Operational implementation of those arrangements will then be difficult and a general lacking of understanding will likely exist in the business and undermine the application process.

## 5. Transaction monitoring and blockchain analysis coverage

Applicants are required to include details of their transaction monitoring procedures which should cover the arrangements in place for monitoring both fiat currency transactions and cryptoasset transactions.

FCA feedback suggests that applicants should be able to demonstrate that their transaction monitoring and blockchain analysis is *"effective"* and *"adequate for its size and complexity"*. This would suggest that applications need to provide a little more detail that just stating what policies and procedures are maintained and which systems are used. Linking to the previously discussed risk content would be a first step, e.g. how have the monitoring policies been set given the assessed risk and how will the procedures and chosen systems work to mitigate the risk. The application should also demonstrate that the monitoring arrangements, including blockchain analysis tools, have adequate coverage of the various types of currencies and transactions.

The FCA's also state that applicants *"must have sufficient compliance resources to monitor transactions, and to carry out alert escalation and treatment*". As discussed in previous guides, the MLRO is a key role within the business, however, the reference to 'compliance resources' indicates that the FCA are looking for staff resources that are commensurate to the size and complexity of the business, i.e. will the MLRO have the time to monitor transaction reports on a day to day basis or will additional support resources be required?

The experience of the MLRO has also previously been highlighted by the FCA and their recent feedback further emphasises that applicants should not have compliance staff that lack the skills to carry out blockchain investigations despite the firms having blockchain analytics tools. The identification and recruitment of good staff, with relevant cryptoasset experience, will take time and should be factored into the application timeline. Staff training should also be emphasised, particularly with regard to cryptoasset issues (see the 'Training' feedback below).

## 6. Group structure and reliance on group policies and procedures

The FCA's feedback reasonably states that applications will not be approved where the applicant *"relies solely on group policies and procedures, but it is unclear how they apply to the applicant"*. This includes not being able to demonstrate how the applicant will comply with the MLR.

Applicants must therefore develop their own approach (i.e. policies and procedures) to comply with regulatory requirements and to appropriately organise the business. This does not preclude 'adopting' group policies where they are suitable for the applicant's business and are aligned with UK requirements. This would help align the applicant's processes with those of the group and thereby facilitate outsourcing arrangements within the group (see below). However, the applicant should not blindly adopt group policies (and procedures) – they should be aligned with the requirements of the applicant's business and be adopted as their own.

Points made by the FCA in their feedback include:

- **Focus on the applicant's business model**. Policies and procedures will need to be specific to the applicant's business. Starting from the business model (service description, service development, forecast size and complexity, etc.) is a logical place to start when considering what policies should be developed, or adopted, and the procedures that will be implemented.
- **Demonstrate how the applicant, key staff and beneficial owners will comply with the MLR**. Ensuring compliance should be the objective of the policies and procedures. They will therefore need to be developed to ensure compliance across the business (inc. staff) and the ownership.

- **Describe the group structure, ongoing activities, jurisdictions and regulatory status**. Where relevant, this information will help set the context for the applicant. Information on the group to which an applicant belongs would help the FCA contextualise the risks faced by the applicant, outsourcing arrangements, potential financial and resource support, etc.

## 7. Outsourcing

Outsourcing is a common feature in regulatory applications and, if properly considered and controlled, should not cause an issue.

Applicants need to provide a description of their outsourcing arrangements, which should include: a description of the outsourced activities and their main characteristics, the identity and geographical location of the outsourcing provider, and the roles (and persons) within the applicant that will be responsible for oversight of the outsourced activities. A description of the way outsourced functions are monitored and controlled (as part of the internal control environment) including the maintenance and operation of an Outsourcing Policy, should also be included. The FCA's feedback suggests that these basic requirements are not being met - feedback from the FCA essentially reiterates these requirements:

- Provide complete information regarding outsourcing arrangements (both within and outside the group, as well as within and outside the UK).
- Maintain robust oversight to ensure that outsourced providers comply with the requirements of the MLR while recognising that the applicant remains ultimately responsible.

Copies of the outsourcing contracts, which may be draft, between the applicant and the service providers are required to be submitted. Applicants should therefore be in a good position to provide the information required above if they have progressed to contractual negotiations and have draft contracts available for submission.

The subject of outsourcing is described in these two guides:

- **Applications for Authorisation: Guide 5 - Outsourcing arrangements**

- **Compliance Arrangements: Guide 4 - Outsourcing arrangements**

FCA feedback also states that they will not approve an application where the applicant fails to provide its policies around outsourcing, fails to demonstrate sufficient oversight of the outsourced activities or fails to evidence that appropriate assurance testing of the outsourced activities will take place. The development of an Outsourcing Policy should help to address these areas of concern, see guide:

- **Compliance Arrangements: Guide 5 - Outsourcing Policy**

## 8. Training

Training is essential for ensuring that key staff are able to perform their designated roles (which would ideally be documented in role-specific Job Description). The focus of the FCA appears to be the 'compliance' staff (see 5 above), ensuring that they have the appropriate skills to carry out their duties. This would encompass the MLRO, who the FCA have repeatedly emphasised, is key to the application process and its success, as well as the supporting 'compliance' staff.

The FCA's feedback states that applicants "*must be able to evidence staff training material tailored to its particular business model and associated AML/CTF risks along with its annual* *training plan”*. Also, where the applicant hires external consultants to develop its AML framework, *“it must demonstrate a comprehensive understanding of this framework and that there is a comprehensive training plan that enables staff to effectively implement the framework”*.

This additional clarification from the FCA is helpful; a reasonable approach to their expectations could therefore involve:

- Training should be driven by the requirements of the particular roles and the individuals performing those roles. The objective would be to ensure that key staff have the required level of knowledge to be ‘fit and proper’ for their roles.
- General ‘awareness’ training, provided to all staff, helps to ensure that general requirements, or at least the background to the regulatory obligations, applicable to the firm and its staff, are understood across the business.
- Training arrangements could reasonably use external materials and courses on certain matters supplemented with bespoke inhouse training specifically tailored to the business (i.e. its services, markets, risks, organisation structure, etc.)
- Initial and ongoing training should be provided. Initial training would be provided upon recruitment in order to get new staff up to speed with their responsibilities, the firm’s operations and arrangements in place to meet regulatory requirements. Ongoing training would be provided to maintain and improve staff knowledge and in the event of a change in the business arrangements, services provided or external factors such as changes in applicable regulation.
- Staff performance assessments. It is advisable to ensure that key staff are subject to ongoing reviews to ensure that they remain fit and proper to perform their designated role. In the event that issues are identified, remedial training should be provided.
- Checks on the provision of training should be included in the Compliance Monitoring Programme.
- As mentioned by the FCA in their feedback, a ‘Training Plan’ should be developed. The plan should detail the performance of general awareness training and ongoing training for all staff and specific training for particular roles / staff (and as informed by the staff reviews).
- A training log should be maintained to record the training provided to each staff member (for record keeping and evidence purposes).

The FCA state that they *“will not approve an application where the applicant has an inadequate training plan or lacks the resources to deliver that training”* and provide examples of issues such as:

- An MLRO with no AML experience attempting to provide inhouse training to staff
- New joiners not being offered training, and
- Staff training completion rates are unsatisfactory.

## 9. <u>Suspicious Activity Reporting</u>

Suspicious Activity Reporting (“SAR”) policies are highlighted by the FCA stating:

- They must fully cover the applicant’s cryptoasset-related activities
- They should not be generic, and

- They should include detailed information about controls on holding cryptoassets that are deemed suspicious and the handling of funds where constraints apply due to blockchain-related processes or attributes.

The development of policies and procedures that are specific to the firm is also covered in section 6 above.

## 10. **Disclosures**

The FCA expect evidence that the applicant will proactively inform customers that the cryptoasset activities will not be within the scope of the Financial Ombudsman Service and will not benefit from the Financial Services Compensation Scheme's protection before establishing a business relationship or entering into a transaction with the customer. This should be included in the Terms of Use and should be covered in website content, Q&A, etc.

## 11. **Applicant is already authorised for other activities**

The FCA state that if the applicant is already registered or authorised (such as an e-money institution, payments institution or a firm with Part 4A permissions under FSMA), it must demonstrate that it understands the requirements of the AML registration regime for cryptoasset businesses. Again, this is a continuation of the theme around the development of specific policies and procedures (for the firm as well as in relation to the services provided).

The FCA state that *"any existing AML framework must be extended to fully cover the new and unique risks of its cryptoasset-related activities"*.

The FCA also state that they *"will consider if the applicant has a history of compliance failings within the existing regime(s) it is subject to"* including *"any ongoing investigations into the applicant, its compliance programme and any backlogs, any unresolved audit findings in its AML/CTF procedures and any regulatory concerns with its transaction monitoring capabilities"*.

## 12. **Sanctions**

The FCA require applicants to evidence *"adequate and current sanctions-specific controls"* within the control framework that are *"in line with its cryptoasset-based business model"*. The FCA specify that the control framework must:

- Include cryptoasset-specific 'red flag' indicators for potential sanctions breaches
- Procedures to ensure that it is kept up to date
- Identification of transactions linked to higher risk wallet addresses that may be associated with a sanctioned entity
- Processes to handle a customer transacting from a sanctioned jurisdiction, and
- Procedures on how to deal with the funds of a designated person.

Evidence that the applicant will apply sanctions checks consistently across various tools and processes, such as onboarding, periodic reviews, transaction monitoring and blockchain analysis, must be included in the application. Again, a *"generic"* sanctions policy will be problematic to the application.

## 13. **Website**

As a final point, the FCA provide feedback on the content of the website and marketing materials:

- *"The applicant's website or other marketing materials must contain an accurate and fair representation of the applicant's products and services and must not contain misleading information".*
- *"The applicant must demonstrate that it has clear oversight and accountability for how third parties use its marketing material, for instance, social media influencers".*

## 14. Key takeaways

Summarised below are some key points that applicant cryptoasset firms might like to consider in order to increase the chances of a successful application:

- Agree a clear service description and understanding of the permissions required.
- Develop a flow of funds diagram detailing the crypto and fiat flows and partners involved.
- Prepare a realistic three-year financial forecast that is consistent with the written content of the application.
- Design a risk management framework and perform a business wide risk assessment that is tailored to the business model.
- Develop a Risk Register to help further the understanding of the risks faced by the business and the mitigating controls that will be operated. This process will assist the preparation of risk narratives in the application, especially when evidencing the assessment of the strength of the mitigating controls.
- Develop and document policies, systems and controls that are bespoke to the firm and its proposed activities.
- Develop a robust AML Framework, specific to the business and services provided.
- Ensure that documents detailing policies and procedures are not generic, underdeveloped or outdated. There must be an emphasis on preparing documents that detail firm-specific arrangements. An understanding of these arrangements must also be demonstrated.
- Develop transaction monitoring processes that cover both fiat and cryptoasset transactions. Applicants should be able to demonstrate that they are effective and adequate for the size and complexity of the business.
- Policies and procedures should be specific to the business. Aligning with group approaches is acceptable provided they comply with UK requirements; in such cases the group's policies and procedures would essentially be 'adopted' by the applicant as their own.
- Staff 'compliance' resources should be sufficient and appropriate to the size and complexity of the business. The MLRO is a key role, however, additional supporting compliance staff may also be necessary.
- Basic outsourcing approaches should be implemented, e.g. clear outsourcing descriptions, contracts, oversight arrangements, monitoring and control arrangements and an Outsourcing Policy.
- Develop staff training materials that are specific to the business and an annual training plan.